LOSCHELDER

Newsletter Datenschutzrecht
September 2021

Sehr geehrte Damen und Herren,

wir melden uns zurück aus der Sommerpause mit einigen besonders praxisrelevanten datenschutzrechtlichen Themen und Neuigkeiten: Der BGH hat das datenschutzrechtliche Auskunftsrecht in einer aktuellen Entscheidung weiter konturiert. Die Auswirkungen dieser Entscheidung und einer Entscheidung des BAG aus April 2021 auf die Beauskunftung von Betroffenenanfragen ist Gegenstand unseres ersten Beitrags. Auf EU-Ebene haben sich gleich mehrere neue Entwicklungen in Sachen Facebook und WhatsApp ergeben, die wir in weiteren Beiträgen beleuchten. Und schließlich gibt es weitere Rechtsprechung zum Schadensersatzanspruch wegen Datenschutzverstößen, die in der Praxis immer häufiger geltend gemacht werden.

Zu guter Letzt haben wir wieder interessante Bußgeld-Entscheidungen für Sie zusammengetragen. Hervorzuheben ist dabei, dass die Datenschutzkommission in Luxemburg im Juli das bisher höchste bekannte Bußgeld wegen DSGVO-Verstößen überhaupt verhängt hat.

Inhalt

DSGVO-Auskunftsanspruch: Mehr Klarheit von BGH und BAG?

Der genaue Inhalt des Auskunftsanspruchs aus Art. 15 DSGVO ist seit Bekanntgabe der DSGVO umstritten. Nach dieser Norm hat jede Person Anspruch auf eine Auskunft darüber, welche personenbezogenen Daten von ihr in einem Unternehmen oder einer Behörde verarbeitet werden. In zwei sehr praxisrelevanten Urteilen haben das Bundesarbeitsgericht und der Bundesgerichtshof den Anspruch nunmehr konturiert. Inzwischen liegen auch die Entscheidungsgründe zu beiden Urteilen vor, so dass bekannt ist, was genau die Gerichte ausgeführt haben. Zu klären war von den Gerichten, ob bei einem Auskunftsverlangen alle in einem Unternehmen vorhandenen Daten, das heißt jede E-Mail, jede irgendwo abgespeicherte Notiz und jede Information über eine Person, herausgesucht und kopiert werden müssen. Nach dem Urteil des Bundesgerichtshofs ist dies der Fall. In längeren vertraglichen Beziehungen können Auskunftsverlangen dadurch enorme Aufwände verursachen. Das Bundesarbeitsgericht hat klargestellt, dass ein derartiger Anspruch sehr genau geltend gemacht werden muss, um durchzugreifen.

In unserem Newsletter vom Mai dieses Jahres berichteten wir bereits von einem Urteil des Bundesarbeitsgerichts (BAG) vom 27.04.2021 – Az.: 2 AZR 342/20 – zum Umfang des Auskunftsanspruchs aus Art. 15 DSGVO. Der Kläger war als Wirtschaftsjurist bei der Beklagten beschäftigt und begehrte Auskunft über seine von der Beklagten verarbeiteten personenbezogenen Daten und Überlassung einer Kopie derselben. Insbesondere wollte der Kläger eine Kopie aller beim Arbeitgeber vorhandenen E-Mails, in denen personenbezogene Daten von ihm enthalten waren.

Das BAG umging im Ergebnis die Beantwortung der Frage, ob auch die Übermittlung von Kopien des E-Mail-Verkehrs des Klägers und aller E-Mails, die ihn namentlich erwähnen, vom Auskunftsanspruch nach Art. 15 DSGVO umfasst ist. Jedenfalls könne ein solcher Anspruch nicht pauschal auf Auskunft über „alle vorhandenen E-Mails“ gestellt werden. Vielmehr müsse der Kläger die E-Mails, auf die er sich beziehe, genau bezeichnen.

Der Bundesgerichtshof (BGH) konnte dagegen dank präziserem Antrag auch in der Sache urteilen: Das Gericht entschied in einem Urteil vom 15.06.2021 – Az.: VI ZR 576/19 -, dass der Anspruch nach Art. 15 DSGVO alle personenbezogenen und personenbeziehbaren Informationen umfasse, die in einem Unternehmen zu einer Person

vorhanden sind. Davon sei auch interne Korrespondenz mit und über den Betroffenen einschließlich der ausgetauschten E-Mails erfasst. Ob die Informationen dem Kläger bereits bekannt sind, sei nicht erheblich. Zweck des Auskunftsanspruchs sei es, den Betroffenen in die Lage zu versetzen, sich zu vergewissern, dass ihn betreffende Daten richtig sind und in zulässiger Weise verarbeitet werden. Anders, als vor dem BAG, ging es hier nicht um einen Arbeitnehmer und seinen Arbeitgeber. Ein Versicherungsnehmer hatte gegenüber der Versicherung Auskunft verlangt.

Das Urteil des BGH dürfte erhebliche Praxisfolgen haben. Schon jetzt nutzen etwa Prüflinge den Auskunftsanspruch aus Art. 15 DSGVO, um eine (unentgeltliche) Kopie ihrer Arbeiten nebst Votum der Prüfer zu erhalten. Max Schrems, der derzeit zum dritten Mal ein umfangreiches Gerichtsverfahren gegen Facebook führt, erhielt unlängst eine Auskunft des Konzerns auf über 1.000 (!) Seiten über von ihm verarbeitete Daten. Auskunftsverlangen in dieser Größenordnung könnten in Zukunft die Regel werden und enorme Ressourcen von Unternehmen binden, da die zu übergebenen Daten im Fall von E-Mails stets auch darauf geprüft werden müssen, ob Geschäftsgeheimnisse oder sonstige vertrauliche Informationen enthalten sind. Nach der DSGVO haben Unternehmen i.d.R. einen Monat Zeit, um Auskunftsverlangen zu beantworten. Die Informationen müssen außerdem kostenlos zur Verfügung gestellt werden. Verweigert werden dürfen Auskunftsersuchen nur bei offenkundig unbegründeten oder exzessiven Anträgen, Art. 12 Abs. 5 DSGVO. Diese Ausnahmen werden bislang eng ausgelegt.

Damit birgt der Anspruch auf Datenauskunft in seiner neuen Ausgestaltung enormes Druck- und Konfliktpotential, auch, um die eigene Position in anderweitigen Auseinandersetzungen zu verbessern. Abzuwarten bleibt daher, unter welchen Umständen die Gerichte Auskunftsverlangen nach Art. 15 DSGVO als rechtsmissbräuchlich einordnen oder dem Anspruch, etwa durch einen Unzumutbarkeitseinwand, Grenzen setzen.

WhatsApp und Facebook reloaded – wie effektiv ist die EU-Abstimmung der Aufsichtsbehörden nach der DSGVO?

Nicht lange ist es her, da regte sich ganz erheblicher Widerstand aus Nutzerkreisen gegen eine Ankündigung von Facebook: Die Nutzungsbedingungen von WhatsApp sollten geändert werden. Mit einer verpflichtenden Datenweitergabe an Facebook. Sichtbare Folge war ein enormer Anstieg der Nutzerzahlen alternativer Angebote wie Threema oder Signal. Und auch die Datenschützer sind aktiv geworden – wieder einmal aus dem hohen Norden: Der Hamburgische Datenschutzbeauftragte leitete ein Dringlichkeitsverfahren ein. Aufgrund des EU-Sitzes der Unternehmen in Irland sind seine Befugnisse begrenzt. Die EU-Gruppierung hat nun ein Einschreiten in dieser Sache abgelehnt. Ein bereits 2018 gegen WhatsApp begonnenes Verfahren wurde dagegen am 02.09.2021 einem Ende zugeführt: die irische Datenschutzbehörde verhängte ein Rekordbußgeld über 225 Mio. Euro. Aber der Reihe nach:

Der Zusammenschluss der europäischen Datenschutzaufsichtsbehörden, der Europäische Datenschutzausschuss (EDSA), hat im Juli 2021 in einer Verbindlichen Entscheidung die Ergreifung von endgültigen Maßnahmen zur Sicherstellung der einheitlichen Anwendung der DSGVO gegenüber WhatsApp und dem Facebook-Konzern abgelehnt (Entscheidung 01/2021, hier abrufbar). Damit

endet ein vom Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) eingeleitetes Dringlichkeitsverfahren über die Untersagung des Datenaustausches zwischen Facebook und WhatsApp.

Unzulässige Datenweitergabe an Facebook?

Wie der HmbBfDI in seiner Pressemitteilung aus April 2021 mitteilte, zielte das Verfahren darauf ab, dem Facebook-Konzern die Weitergabe und Nutzung der über den Messenger-Dienst WhatsApp gesammelten Daten zu eigenen Zwecken zu untersagen. Zurück ging dies auf die Ankündigung des Konzerns Anfang 2021, die Nutzungsbedingungen und Datenschutzbestimmungen des Konzerns dahingehend zu ändern, dass die Weitergabe dieser Daten an die übrigen Unternehmen des Facebook-Konzerns, etwa die Plattformen Facebook und Instagram, zulässig ist. Die weitere Nutzung von WhatsApp wurde von der Akzeptanz der geänderten Nutzungsbedingungen abhängig gemacht.

Der HmbBfDI äußerte die Befürchtung, durch den erweiterten Datenaustausch könnten die Daten nicht nur für Produktverbesserungs- und Analysezwecke, sondern auch für Marketing und Direktwerbung genutzt werden. Die deutsche Datenschutzaufsichtsbehörde kritisierte auch, dass die federführend zuständige irische Datenschutzaufsichtsbehörde bisher den Datenaustausch zwischen WhatsApp und dem Mutterkonzern nicht genauer untersucht hätte. In der Kombination sah der HmbBfDI die Möglichkeit der unzulässigen Durchsetzung eines massenhaften Datenaustauschs und leitete deshalb ein Dringlichkeitsverfahren nach Art. 66 Abs. 1 DSGVO ein. Dieses fand seinen Abschluss mit einem vorläufigen Verbot der Weiterverarbeitung der WhatsApp-Nutzerdaten deutscher Kunden durch den Facebook-Konzern (Pressemitteilung).

Das Dringlichkeitsverfahren nach Art. 66 Abs. 1 DSGVO stellt ein Mittel zum kurzfristigen Einschreiten von Aufsichtsbehörden dar, die einen dringenden Handlungsbedarf zum Schutz der Rechte und Freiheiten von Betroffenen sehen. Hierzu können die Aufsichtsbehörden für ihren Zuständigkeitsbereich einstweilige Maßnahmen mit einer Geltungsdauer von höchstens drei Monaten erlassen. Dabei ist der HmbBfDI nur für Deutschland die für den Facebook-Konzern zuständige Aufsichtsbehörde; die federführende Aufsicht hat die irische Datenschutzaufsichtsbehörde, die Data

Protection Commission (DPC), inne. DPC und Facebook konnten zum Vorgehen des HmbBfDI sodann umfassend Stellung nehmen, bevor der EDSA über die Verhängung endgültiger, bindender Maßnahmen zu entscheiden hatte.

Unzureichende Informationen für endgültige Entscheidung

Der EDSA hat nun mit der Verbindlichen Entscheidung 01/2021 im Juli 2021 die endgültige Entscheidung in diesem Verfahren getroffen: Es werden keine Maßnahmen gegen Facebook ergriffen. Zwar vermutete der EDSA, dass der Facebook-Konzern und WhatsApp die über WhatsApp gesammelten Nutzerdaten als gemeinsame Verantwortliche für jeweils eigene Zwecke auch schon vor der Änderung der Nutzungsbedingungen verarbeiteten. Auch bei der derzeitigen Datenweitergabe und -verarbeitung zwischen den Konzernen sieht der EDSA die Möglichkeit eines DSGVO-Verstoßes als gegeben. Weil aber bisher keine umfassende Untersuchung der Verarbeitungspraxis durchgeführt wurde, fehlte es dem EDSA an eindeutigen Informationen, sodass ein Verstoß gegen die DSGVO nicht mit Sicherheit angenommen werden konnte. Deshalb wurden keine endgültigen Maßnahmen gegen die Unternehmensgruppe ausgesprochen.

Kontrollauftrag für DPC

Damit steht indes weiterhin nicht fest, dass das Verhalten von Facebook und WhatsApp datenschutzrechtlich zulässig ist. Es mangelte aus Sicht des EDSA lediglich an Nachweisen für einen DSGVO-Verstoß. Folgerichtig gab der EDSA denn auch der zuständigen DPC auf, eine Untersuchung der Datenverarbeitung zwischen WhatsApp und dem Facebook-Konzern durchzuführen. Sollte diese zu dem Ergebnis kommen, dass tatsächlich ein Verstoß gegen die DSGVO-Vorschriften vorliegt, wären umfassende Aufsichtsmaßnahmen zu ergreifen.

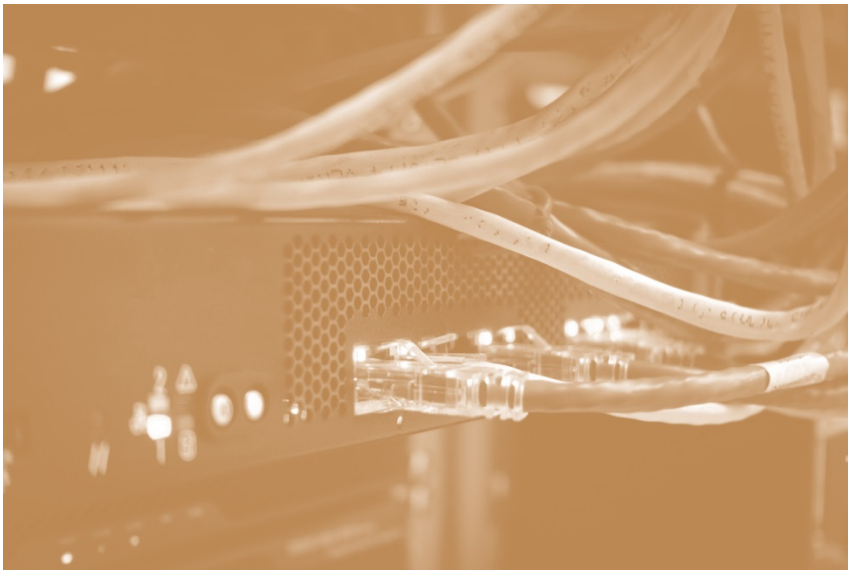
Rekordbußgeld gegen WhatsApp aufgrund EDSA-Beschlusses

Dass diese – wenn auch nach langen Verfahren – zu erheblichen Konsequenzen führen können, zeigt ein jüngst erlassenes Bußgeld gegen WhatsApp. Die irische Datenschutzbehörde hat am 02.09.2021 ein bereits 2018 begonnenes Verfahren gegen WhatsApp beendet und ein Rekordbußgeld über 225 Mio. Euro gegen WhatsApp erlassen. Es handelt sich um das höchste Bußgeld, das von der

irischen Datenschutzbehörde erlassen wurde. EU-weit belegt es den zweiten Rang: nur die luxemburgische Datenschutzkommission hat mit einem Bußgeld über 746 Mio. Euro gegen Amazon eine höhere Geldbuße verhängt (dazu auch unten im „Zu guter Letzt“).

Das Bußgeld gegen WhatsApp erging aufgrund eines Verbindlichen Beschlusses des EDSA, dieses Mal in einem Kohärenzverfahren nach Art. 65 Abs. 1 DSGVO. Nach Inkrafttreten der DSGVO erreichten die irische Datenschutzbehörde verschiedene Beschwerden über Datenverarbeitungspraktiken bei WhatsApp. Bemängelt wurde dabei die Einhaltung der Transparenzverpflichtungen bei der Übertragung von personenbezogenen Daten zwischen WhatsApp und diversen Facebook-Unternehmen. Im Dezember letzten Jahres übermittelte die irische Datenschutzbehörde ihren Entscheidungsentwurf in dieser Sache zur Prüfung an weitere europäische Datenschutzbehörden, um einen europäischen Konsens herbeizuführen. Da dieser zunächst ausblieb, wurde der Fall anschließend an den Europäischen Datenschutzausschuss überwiesen. Am 28.07.2021 nahm dieser eine verbindliche Entscheidung in der Sache an, die der irischen Datenschutzbehörde mitgeteilt wurde. Die Entscheidung enthielt klare Anweisungen, die von den Iren vorgeschlagene Geldbuße zwischen 30 und 50 Millionen Euro neu zu bewerten und zu erhöhen, woraufhin die Datenschutzbehörde eine Geldbuße i.H.v. 225 Mio. Euro gegen WhatsApp wegen fehlender Transparenz bei der Weitergabe von persönlichen Daten gem. Art. 5, 12, 13, 14 DSGVO verhängte. Außerdem wurde der Messenger-Dienst angewiesen, seine Datenverarbeitung durch Abhilfemaßnahmen in Einklang mit der DSGVO zu bringen.

WhatsApp erklärte, rechtlich gegen die Entscheidung vorgehen zu wollen. Das Ergebnis eines solchen Verfahrens bleibt abzuwarten. Schon häufig wurden Geldbußen wegen Datenschutzverstößen im Rahmen anschließender Gerichtsverfahren erheblich reduziert.



Facebook und Datenschutz – Erneut Schrems-Klage vorm EuGH

Die Verarbeitung personenbezogener Daten durch Facebook wird abermals den EuGH beschäftigen: Der österreichische Oberste Gerichtshof (OGH) legt Europas höchstem Gericht eine Reihe von Fragen zu der Vereinbarkeit der Nutzungsbedingungen der Plattform mit der DSGVO vor. Der Beantwortung der Vorlagefragen durch den EuGH könnte grundlegende Bedeutung auch für eine Vielzahl anderer Bereiche des Datenschutzes zukommen. Im Kern steht auf dem Prüfstand, welche Verarbeitungsvorgänge Gegenstand eines Vertrages sein können und wann eine Einwilligung alternativlos ist. Wir stellen die Hintergründe und Aussichten des Verfahrens in diesem Beitrag vor.

In den letzten Jahren ist vielen der Name Maximilian Schrems ein Begriff geworden: Der österreichische Jurist und Datenschützer ist vor allem wegen seiner Klagen gegen die Datenverarbeitungspraxis des Internetriesen Facebook bekannt – über die sogenannten Schrems I und -II-Urteile berichteten wir unter anderem in unseren Newslettern aus Januar 2020 sowie August 2020. Die Folgen dieser Entscheidungen sind in der Praxis umfassend spürbar: Der Datentransfer in die USA ist nur noch unter erschwerten Bedingungen, wenn überhaupt, datenschutzkonform möglich. Jüngst richtete Schrems mit der Organisation NOYB das Augenmerk auch auf die Ausgestaltung von Cookie-Bannern – darüber berichteten wir im Juni 2021.

In einem weiteren Verfahren vor österreichischen Gerichten griff Maximilian Schrems gemeinsam mit seiner Datenschutz-NGO NOYB umfassend die Datenverarbeitung der Nutzerdaten auf Facebook an. Wie das online-Magazin heise.de erklärt, ging es ganz grundsätzlich um die Frage, ob Facebook bei der Verarbeitung von Nutzerdaten gegen die Vorgaben der DSGVO verstößt. Nun hat der österreichische Oberste Gerichtshof (OGH) einen vorläufigen Schlusspunkt in diesem Verfahren gesetzt: Zum einem wurde Maximilian Schrems ein „symbolisches Schmerzensgeld" von 500 Euro zuerkannt, zum anderen wurden dem EuGH eine Reihe von Fragen vorgelegt (Rechtssache 6 Ob 56/21k – auszugsweise Veröffentlichung durch NOYB – Vorlagefragen, Entscheidung über das Schmerzensgeld).

OGH legt dem EuGH Fragen zur Klärung vor – Einwilligung oder Nutzungsvertrag

Kernanliegen des OGH ist es, zu klären, ob Facebook seine Nutzungsbedingungen DSGVO-konform ausgelegt hat. Wie NOYB auf ihrer Website darstellt, interpretiert Facebook nämlich seit der Anwendbarkeit der DSGVO im Mai 2018 die „Einwilligung" ihrer Nutzer in die Datenverarbeitung als Abschluss eines Vertrages – mit der Konsequenz, dass die Nutzer aus Sicht von Facebook personalisierte Werbung „bestellen" würden. Weil nun ein Vertrag zwischen Facebook und den Nutzern vorläge, gelten die strengen Anforderungen, die die DSGVO an die Einwilligung stellt, nicht. Insbesondere die in Art. 6 Abs. 1 UAbs. 1 lit. a, Art. 7 DSGVO aufgestellten Erfordernisse der Freiwilligkeit, Informiertheit und Bestimmtheit der Einwilligung müssten deshalb nicht mehr beachtet werden.

Maximilian Schrems und NOYB zweifeln daran, ob dies mit der DSGVO vereinbar ist und kritisieren, dass Facebook versucht, die Voraussetzungen der DSGVO zu umgehen. Der OGH teilt die Zweifel und gab sie an den EuGH weiter. Dieser wird nun zu klären haben, ob

- die Verarbeitung von personenbezogenen Daten zu Zwecken der personalisierten Werbung auf Plattformen nur auf der Grundlage einer Einwilligung im Sinne des Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO erfolgen darf oder auch ein Vertrag als Verarbeitungsgrundlage im Sinne des Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO herangezogen werden kann.

- Facebook mit der umfassenden Aggregierung von personenbezogenen Daten gegen die Grundsätze der Datenminimierung nach Art. 5 Abs. 1 lit. c DSGVO verstößt. Facebook führt eine Vielzahl von Daten, die auf der Plattform selbst oder auf anderen Websites, etwa über Like-Buttons, gesammelt wurden, ohne Einschränkung nach Zeit oder Art der Daten zusammen und nutzt diese Daten für zielgerichtete Werbung.

- Art. 9 Abs. 1 DSGVO, der die besondere Schutzwürdigkeit bestimmter Kategorien von Daten wie die politische Überzeugung oder die sexuelle Orientierung bestimmt, auch dann zum Tragen kommt, wenn Daten ohne Differenzierung gesammelt, aggregiert und für die Schaltung personenbezogener Werbung eingesetzt werden. Art. 9 Abs. 2 DSGVO stellt besondere Anforderungen an die Verarbeitung der Daten, die unter Art. 9 Abs. 1 DSGVO fallen, was auch bei der Aggregation und Verarbeitung zum Zweck der personalisierten Werbung relevant werden könnte.

Die Beantwortung insbesondere der ersten Frage kann weit über den Social Media-Bereich hinaus Bedeutung erlangen: Die Frage, ob eine bestimmte Datenverarbeitung auf vertraglicher Grundlage erlaubt werden kann oder eine Einwilligung erforderlich ist, stellt sich immer wieder in unterschiedlichen Lebensbereichen.

Symbolisches Schmerzensgeld für Maximilian Schrems wegen „Ostereiersuche“

Neben dem Vorlagebeschluss erließ der OGH noch ein Teilurteil, in dem Facebook zur Zahlung eines symbolischen Schmerzensgeldes an Maximilian Schrems i.H.v. 500 Euro verurteilt wird. Damit soll ausgeglichen werden, dass Facebook Schrems auf Anfrage nicht, wie in der DSGVO vorgesehen, alle vom Netzwerk verarbeiteten personenbezogenen Daten zur Verfügung gestellt hatte, sondern eine Eigeneinschätzung über die „relevanten“ Daten vornahm und nur diese übermittelte.

Auch die Art und Weise, wie der Konzern die Auskunft erteilte, spielte für das Schmerzensgeld eine Rolle: Wie die österreichische Zeitung Der Standard berichtete, verglich der Gerichtshof das über 1.000 Seiten lange Dokument mit mindestens 60 Datenkategorien und einer Vielzahl von Datenpunkten mit einer „Ostereiersuche“. Auch dies sei nicht mit der DSGVO vereinbar.

Schrems III in Aussicht?

Mit der Vorlageentscheidung des OGH rückt eine Schrems III-Entscheidung in greifbare Nähe. Diesmal steht indes nicht der US-Transfer, sondern die Reichweite verschiedener Erlaubnisgrundlagen der DSGVO auf dem Prüfstand. Dabei zeigen sich beide Seiten kämpferisch: Auf der NOYB-Website prognostiziert Maximilian Schrems, dass die Niederlage von Facebook vorm EuGH zur Pflicht zur Datenlöschung und Schadensersatzverpflichtungen gegenüber Millionen von Facebook-Nutzern führen könnte – und zeigt sich entsprechend glücklich mit der Vorlageentscheidung. Ähnlich selbstsicher gibt sich ein Facebook-Sprecher gegenüber dem Nachrichtendienst Reuters und erinnert daran, dass der Konzern bereits erhebliche Veränderungen hin zur besserer Transparenz und einer größeren Kontrolle der Nutzer über ihre Daten unternommen habe.

Welchen Schaden können Betroffene bei einem Datenschutzverstoß geltend machen?

Ein Verstoß gegen DSGVO und nationales Datenschutzrecht kann – jenseits der vielbesprochenen Bußgelder – auch zu einem Schadensersatzanspruch Betroffener führen. Art. 82 DSGVO enthält einen solchen Anspruch. In der Praxis wird dieser immer häufiger geltend gemacht. Die Gerichte haben daher zunehmend Gelegenheit, Voraussetzungen und Grenzen zu konkretisieren.

Ohne Schadensvortrag gibt es auch bei einem Datenschutzverstoß keinen Schadensersatz: Der Schadensersatzanspruch gem. Art. 82 Abs. 1 DSGVO setzt voraus, dass einer natürlichen Person wegen eines Verstoßes gegen das Datenschutzrecht ein materieller oder immaterieller Schaden entstanden ist. Das Oberlandesgericht Bremen hat dazu jüngst bestätigt (E. v. 16.07.2021, 1 W 18/21):

Die Behauptung eines Verstoßes gegen die Vorschriften der DSGVO allein genügt nicht. Der Anspruchsteller muss auch den hierdurch kausal entstandenen materiellen und / oder immateriellen Schaden darlegen und beweisen. Der Wortlaut des Art. 82 DSGVO zeige insoweit eindeutig, dass ein solcher Vortrag notwendig sei. Betont wurde auch, dass nicht etwa die Frage der Erheblichkeit des Schadens im Raum stünde (dazu hat das BVerfG unlängst den EuGH angerufen mit der Frage, ob bei Bagatellschäden ein Ersatzanspruch ausgeschlossen sei, wir berichteten hier). Vielmehr stünde einem Anspruch der Antragstellerin schlicht und ergreifend entgegen, dass es bereits an jeglichem Vorbringen hinsichtlich eines durch die Rechtsgutsverletzung geltend gemachten Schadens fehle.

Auch das OLG Stuttgart hatte vor nicht allzu langer Zeit den Ansatz Betroffener verworfen, aufgrund der Rechenschaftspflicht der Unternehmen würden die üblichen Darlegungs- und Beweislastregeln beim DSGVO-Schadensersatz nicht gelten. Im Gegenteil: Auch ein DSGVO-Schadensersatzanspruch muss vollumfänglich dargelegt und der Beweis geführt werden (wir berichteten hier).

Und noch eine interessante Entwicklung zeichnet sich ab: Das Bundesarbeitsgericht (BAG) hat Ende August dem EuGH zwei zentrale Fragen zu Umfang und Reichweite des DSGVO-Schadensersatzes vorgelegt (E. v. 26.08.2021, 8 AZR 253/20 (A)): Zum einen stellt das BAG zur Bemessung der Schadenshöhe die Frage nach dem spezial- und generalpräventiven Charakter des Anspruchs und, ob dieser zu berücksichtigen sei. Zum anderen fragt das BAG – ebenfalls zur Schadenshöhe bei immateriellen Schäden –, ob es auf den Grad des Verschuldens ankommt. Üblich ist dies jenseits der Vorschriften zum Mitverschulden, um die es hier aber nicht geht, nicht.

Zu guter Letzt

Diesen Monat warten Datenschutzbehörden europaweit mit Bußgeldbescheiden in Millionenhöhe auf. Bemerkenswert ist insbesondere die Verurteilung des Unternehmens Amazon Luxemburg, gegen welches der höchste Bußgeldbescheid seit Inkrafttreten der DSGVO am 25.05.2018 verhängt wurde. Gespannt sein dürfen Sie auch auf Entscheidungen bezüglich Monsanto und der weltweit durchschlagenden Social-Media-App TikTok sowie auf eine datenschutzrechtliche Bewertung der Verwendung biometrischer Systeme in Supermärkten.

- **746.000.000 Euro Bußgeld gegen Amazon**

Die nationale Datenschutzbehörde verhängte gegen Amazon Europe Core S.à.r.l mit Sitz in Luxemburg ein enormes Bußgeld i.H.v. 746 Mio. Euro. Dies steht im Zusammenhang mit der von der französischen Bürgerrechtsorganisation „La Quadrature du Net“ eingereichten Beschwerde von 2018. Details dazu, welche Verstöße Amazon vorgeworfen werden, sind noch nicht bekannt. Amazon hat aber bereits angekündigt, gegen dieses mit Abstand höchste Bußgeld, das seit Inkrafttreten der DSGVO erlassen wurde, vorgehen zu wollen.

- **Spanien: Bußgeld i.H.v. 2,52 Mio. Euro für Supermarktkette**

Die Supermarktkette Mercadona benutzte ein Videoüberwachungssystem, das mit Gesichtserkennung arbeitete, um Personen zu identifizieren, die in einer ihrer Filialen Straftraten begangen hatten und deshalb einem Hausverbot unterworfen waren. Aufgrund eines Verstoßes gegen Art. 5 Abs. 1 lit. c, 6 Abs. 1, 9 Abs. 1, 12, 13, 25 Abs. 1 und 35 DSGVO erlegte die spanische Datenschutzbehörde dem Supermarkt ein Bußgeld i.H.v. ursprünglich 3,15 Mio. Euro auf, welches dann auf 2,52 Mio. Euro reduziert wurde.

Das System verglich eines oder auch mehrere Bilder einer Person mit einer Datenbank biometrischer Muster, die bereits mit der Identität der Person in Verbindung gebracht wurden. Die Datenverarbeitung beinhaltete die Erfassung, den Abgleich, die Speicherung und – im Falle einer negativen Identifizierung 0,3 Sekunden nach der Erfassung – die Vernichtung des erfassten biometrischen Bildes jeder Person, die den Supermarkt betrat. Da Gesichtserkennungssysteme besonders invasiv in die Rechte und Freiheiten der Betroffenen eingreifen, handele es sich bei den biometrischen Daten um besondere Daten gem. Art. 9 DSGVO. Da das System außerdem automatisch unter Verwendung von Algorithmen arbeite, sei das Risiko einer willkürlichen und massenhaften Überwachung hoch. Ein öffentliches Interesse an der Verarbeitung sei mangels entsprechender Normierung im nationalen Recht nicht gegeben. Darüber hinaus war der Händler weder in der Lage nachzuweisen, dass sich die Verarbeitung auf die minimal erforderlichen Daten beschränkte, noch hatte er technische Schutzvorrichtungen eingerichtet, um die Rechte und Freiheiten der Betroffenen zu schützen. Trotz des hohen Risikos hatte eine Datenschutzfolgenabschätzung ebenso gefehlt wie eine Aufklärung der Betroffenen über die Verarbeitung ihrer personenbezogenen Daten.

Erschwerend wurde zudem berücksichtigt, dass hier besondere Kategorien personenbezogener Daten verarbeitet wurden und dass auch Minderjährige sowie weitere vulnerable Gruppen betroffen waren.

- **Frankreich: Bußgeld gegen Monsanto im Rahmen des Glyphosat-Diskurses**

Monsanto speicherte personenbezogene Daten wie Organisation und Position, Geschäftsadresse und geschäftliche Telefonnummer, Mobiltelefonnummer, geschäftliche E-Mail-Adresse oder auch Twitter-Accounts von Personen, die den Diskurs und die öffentliche Meinung über eine Erneuerung des von Monsanto produzierten Unkrautvernichtungsmittels Glyphosat beeinflussen konnten. Betroffen waren mehr als 200 politische Persönlichkeiten sowie auch Mitglieder der Zivilgesellschaft. Flankiert wurde die Speicherung der Daten von einer Bewertung auf einer Skala von eins bis fünf bezüglich des Einflusses, der Glaubwürdigkeit und der Unterstützung der Person für Monsanto. Eine Information der Betroffenen über die Speicherung ihrer Daten unterblieb bis zu dem Zeitpunkt, zu dem die Medien den Vorgang bereits aufgedeckt hatten. Zwar sei eine Zustimmung der Betroffenen nicht erforderlich gewesen, die Betroffenen sollten aber dennoch in die Lage versetzt werden, ihre Rechte wahrnehmen zu können. In der Folge erließ die Datenschutzbehörde ein Bußgeld i.H.v. 400.000 Euro gegen das Unternehmen.

- **Niederlande: Konsequenzen für die Social-Media-App TikTok**

In den Niederlanden verwenden über 3,5 Mio. Personen TikTok, hierunter auch viele Minderjährige und kleine Kinder. Initiative Untersuchungen der niederländischen Datenschutzbehörde ergaben, dass die den Nutzern zur Verfügung gestellte Datenschutzerklärung ausschließlich in englischer Sprache verfasst war, was für Kinder nicht oder jedenfalls nicht leicht verständlich ist. Hierin sah die Behörde eine Verletzung der Informationspflicht des Unternehmens und belegte das Unternehmen mit einem Bußgeld i.H.v. 750.000 Euro. Kurios an dem Sachverhalt war die Begründung einer Niederlassung von TikTok in Irland noch im Laufe der Ermittlungen. Der Hauptsitz des Unternehmens befindet sich außerhalb der EU. Ab dem Zeitpunkt der Begründung der Niederlassung war die niederländische Datenschutzbehörde nur noch dazu befugt, die Datenschutzerklärung des Unternehmens zu bewerten, da darin enthaltene Verstöße in der Vergangenheit lagen. Zugunsten einer Weiterführung der Ermittlungen gegen TikTok wegen weiterer zweifelhafter datenschutzrechtlicher Praktiken

übermittelte die niederländische Datenschutzbehörde ihre Untersuchungsergebnisse deshalb an die irische Datenschutzbehörde.

- **Italien: 2 Mio. Euro gegen Deliveroo**

Der Bußgeldbescheid gegen den größten in Italien tätigen Lieferdienst steht im Zusammenhang mit Inspektionen zum Umgang mit Arbeitnehmerdaten. Hauptaugenmerk waren speziell die ca. 8.000 Fahrer als Betroffene. Der Lieferdienst verwendete zur Verwaltung der Fahrer ein zentralisiertes System, mit dem die Fahrer via App verbunden waren. In dieser App mussten sie Telefonnummer und E-Mail-Adresse verknüpfen. Probleme ergaben sich hinsichtlich der verwendeten Algorithmen, bei denen das Unternehmen nicht die Genauigkeit oder Korrektheit der Ergebnisse gewährleistete und die betroffenen Arbeitnehmer nicht hinreichend informierte. Auch ein System zum Schutz des Rechts auf menschliches Eingreifen, Meinungsäußerung oder Anfechtung der Entscheidungen der App wurde nicht etabliert. Darüber hinaus sei gegen die Prinzipien der Datenminimierung, Speicherbegrenzung und Zweckbindung der Verarbeitung verstoßen worden. Die Standortdaten der Fahrer wurden etwa alle 12 Sekunden erfasst und zusammen mit anderen persönlichen Daten gespeichert. Auch die Speicherdauer wurde nicht angemessen definiert: Das Unternehmen gab an, dass personenbezogene Daten stets sechs Jahre gespeichert würden. Weiterhin fehlten technische und organisatorische Schutzvorrichtungen sowie eine Datenschutzfolgenabschätzung.

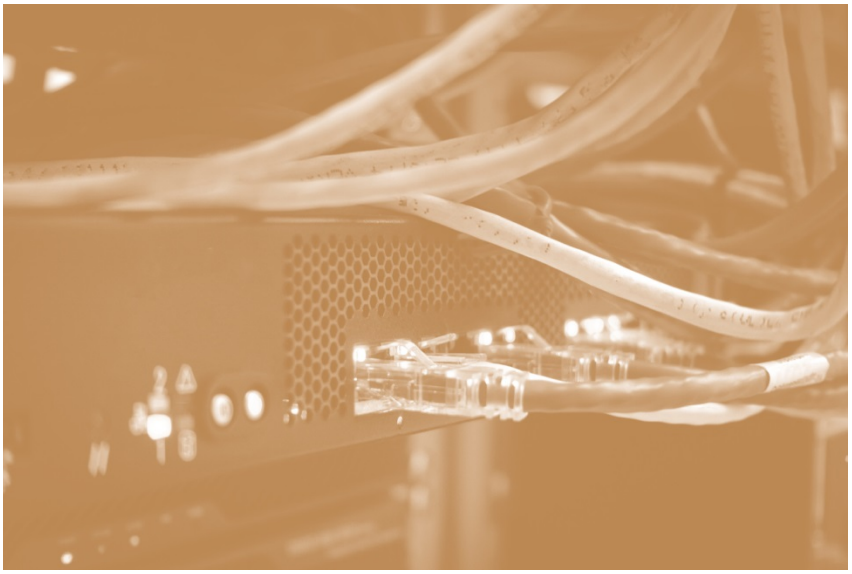
- **Österreich: Bußgeld wegen Profilings beim Kundenbindungsprogramm**

Die österreichische Tochter von REWE – Unser Ö-Bonus Club GmbH – betreibt ein Kundenbindungsprogramm, in dessen Rahmen sie individuelle Kundenprofile zugunsten eines zielgenauen Marketings erstellte (sog. „Profiling“). Dies sei von der im Anmeldeformular enthaltenen Einwilligungserklärung der Kunden nicht hinreichend verständlich erfasst, da die diesbezüglichen Informationen zur Datenverarbeitung nicht vor, sondern nach dem Kästchen zur Einwilligung platziert worden waren. Bei physischen Anmeldeformularen wurde der Anschein erweckt, es handele sich lediglich um eine Bestätigung der Anmeldung zum Programm. Hierdurch sei gegen die Informationspflicht des Unternehmens

verstoßen worden, die Einwilligung sei in der Folge ungültig. Bei der Festsetzung des Bußgeldes i.H.v. 2 Mio. Euro wurden finanzielle Härten durch die COVID-19-Pandemie mildernd berücksichtigt.

- **Frankreich: 1,75 Mio. Euro gegen nationalen Privatversicherer**

Ein Unternehmen der Unternehmensgruppe AG2R LA MONDIALE, einem französischen Privatversicherer mit Sitz in Paris, speicherte personenbezogene Daten von Millionen Personen über einen übermäßig langen Zeitraum und verstieß somit gegen das Prinzip der Speicherbegrenzung. Aufgabe des Unternehmens war die Koordinierung des Vorsorge-, Abhängigkeits-, Kranken-, Spar- und Zusatzrentenversicherungsgeschäfts der Gruppe. Auch die Informationspflicht des Unternehmens sah die Datenschutzbehörde als verletzt an, da Betroffene im Rahmen telefonischer Akquisekampagnen nicht ordnungsgemäß aufgeklärt worden waren. Telefonate wurden bspw. ohne Information diesbezüglich und ohne Widerspruchsmöglichkeit aufgezeichnet. In der Folge verhängte die französische Datenschutzbehörde gegen den Privatversicherer ein Bußgeld i.H.v. 1,75 Mio. Euro.



Für alle weiteren Fragen rund um das Datenschutzrecht stehen Ihnen gerne zur Verfügung

Dr. Kristina Schreiber
+49(0)221 65065-337
kristina.schreiber@loschelder.de

Dr. Simon Kohm
+49(0)221 65065-200
simon.kohm@loschelder.de

Dr. Malte Göbel
+49(0)221 65065-337
malte.goebel@loschelder.de

Impressum

LOSCHELDER RECHTSANWÄLTE
Partnerschaftsgesellschaft mbB
Konrad-Adenauer-Ufer 11
50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110
info@loschelder.de
www.loschelder.de